# Penetration Testing SmartHouse Aplikacije

## BSEP – 2023

Za penetraciono testiranje veb i serverskih aplikacija SmartHouse projekta korišćeni su sledeći alati: *Nmap, Burp Suite i sqlmap* .

**Nmap (Network mapper)** je široko rasprostranjen, *open-source* alat koji se koristi za pregled i skeniranje mreže. Njegova glavna uloga je da pronađe *hostove*, otvorene *portove,* kao i servise koji su pokrenuti na mreži. Glavni alat u okviru Nmapa koji je korišćen za pronalazak ranjivosti je **NSE – Nmap Scripting Engine**, koji omogućava korisnicima da pišu skripte, kao i da pokreću već postojeće skripte, pomoću kojih mogu da se vrše specifični testovi i provere.

Za potrebe ovog testiranja, odabrano je nekoliko skripti koje se često koriste za detekciju nekih od najčešće prisutnih ranjivosti i “rupa” u sistemu.

#### SSL Known Key

SSL-Known-Key se koristi za proveru SSL/TLS sertifikata u odnosu na statičku listu javno dostupnih *key fingerprintova*. Ukoliko su SSL sertifikati povezani sa nekim od poznatih, javno dostupnih ključeva, to može biti indikator da sistem nije dobro konfigurisan i može predstavljati potencijalan bezbednosni problem.

Očekivano, izvršavanjem ove skripte ustanovljeno je da sertifikat koji je generisan za potrebe ovog projekta nije kompromitovan.

#### HTTP SQL Injection

HTTP-SQL-Injection se koristi za detekciju SQL Injection ranjivosti u web aplikacijama koje koriste HTTP protokol. Ova skripta šalje specijalno dizajnirane zahteve i analizira odgovore u potrazi za nedostacima u sistemu koji bi omogućili SQL Injection napade.

SQL Injection napadi se mogu dogoditi ako se korisnički podaci ne validiraju i ne izvrši adekvatna sanitizacija. Cilj je izvršavanje malicioznih komandi nad bazom podataka koju sistem koristi.

Izvršavanjem ove skripte, nisu pronađene tačke u aplikacijama koje bi mogle da propuste maliciozne unose, što znači da je aplikacija bezbedna u kontekstu SQL napada.

#### HTTP Cookie Flags

HTTP Cookie Flags je skripta koja služi za identifikaciju sigurnosnih i konfiguracionih propusta povezanih sa upotrebom kolačića na web serverima. Ona šalje zahteve ka serveru, a potom analizira zaglavlja odgovora u potrazi za kolačićima. Nakon toga, vrši se evaluacija pronađenih kolačića.

Izvršavanjem ove skripte, ustanovljeno je da su kolačići dobro konfigurisani, tj. da su prisutna sva zaglavlja koja služe da bezbednost sistema bude na maksimalnom nivou.

#### HTTP Internal IP Disclosure

HTTP Internal IP Disclosure je skripta koja se koristi za detekciju “curenja” internih IP adresa. Skripta šalje HTTP zahteve ka sistemu, a potom analizira odgovor u potrazi za internim IP adresama sistema. Otkrivanjem internih IP adresa, napadač bi stekao korisne informacije o infrastrukturi mreže, na osnovu kojih bi mogao da bolje planira buduće napade.

Izvršavanjem ove skripte potvrđeno je da ovakvi propusti nisu prisutni u aplikaciji.

#### HTTP Password (HTTP Passwd)

HTTP Passwd je skripta koja se koristi za ekstrakciju i preuzimanje *hash*-eva lozinki iz sistema zasnovanih na HTTP autentifikaciji. Skripta funkcioniše tako što analizira odgovore sistema u potrazi za *hash* lozinkama, na osnovu kojih bi napadač mogao da snabde neke druge alate za otkrivanje lozinki, kao i da ustanovi bezbednosne zahteve koje sistem poseduje prilikom definisanja lozinki (to može da smanji skup potencijalnih lozinki koje bi napadač morao da proveri).

Izvršavanjem ove skripte ustanovljeno je da SmartHouse sistem bezbedno sladišti sve autentifikacione kredencijale.

#### HTTP CSRF

HTTP CSRF je skripta koja služi za otkrivanje ranjivosti u sistemu povezanih sa CSRF napadima. Cilj ovih napada je da se zloupotrebi autentifikacija korisnika, tj. da prinudno izvrše zahtevi ka web serveru koristeći autentifikaciju korisnika bez njegovog znanja.

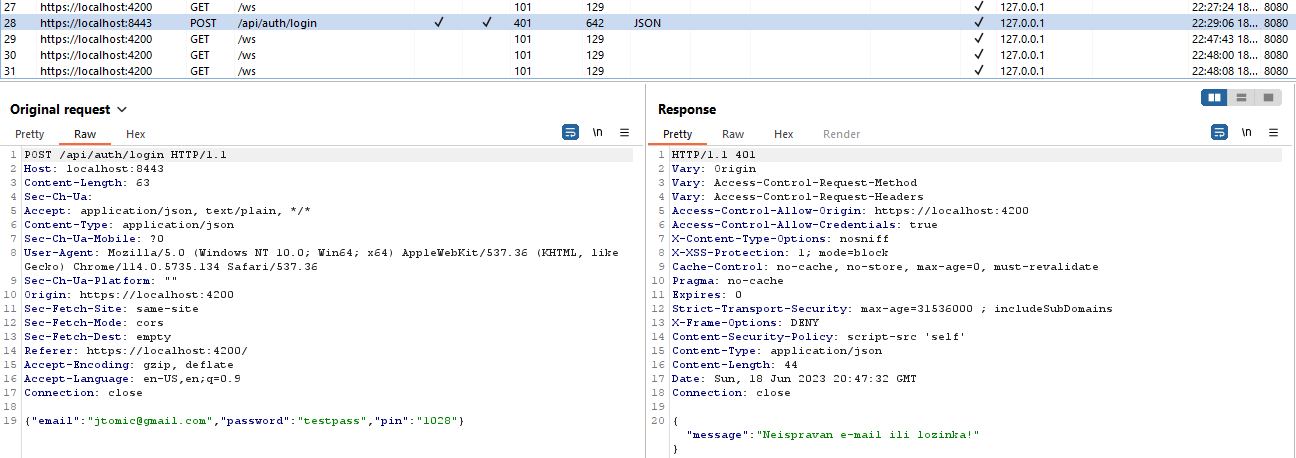
Pokretanjem ove skripte, ustanovljeno je da ne postoje očigledni propusti koji bi omogućili ovakve napade.

**Burp Suite i SQLMap**

**Burp Suite** predstavlja skup alata koji se koriste za testiranje sigurnosti web aplikacija. Burp Suite sadrži niz funkcionalnosti koje pomažu u identifikovanju ranjivosti u aplikacijama i izvršavanju penetracionog testiranja. Dva najvažnija alata unutar Burp Suite-a su *Proxy* i *Intruder*, alat *Proxy* je korišćen prilikom penetracionog testiranja naše aplikacije. *Burp Suite Proxy* funkcioniše kao posrednik između klijenta i servera. Omogućava nam da uhvatimo, manipulišemo i pregledamo kompletan saobraćaj između pregledača i ciljne aplikacije. Daje nam mogućnost analize i izmene HTTP zahteva i odgovora.

**SQLMap** je open-source alat za automatizaciju penetracionog testiranja baziranog na SQL injekcijama. Namenski je razvijen za otkrivanje i iskorišćavanje ranjivosti koje proizilaze iz neadekvatne obrade SQL upita u web aplikacijama. SQLMap automatski prepoznaje različite vrste SQL injekcija, pronalazi ranjive tačke i omogućava izvršavanje različitih vrsta SQL baziranih napada kako bismo testirali sigurnost aplikacije.

Na samom početku testiranja presretali smo zahteve upućene sa klijentske strane, to su uglavnom bili zahtevi koji se šalju serverskoj strani nakon popunjavanja neke forme. Ovakvi zahtevi su najpogodiniji za izvršavanje SQL napada.



Ilustracija 1 Prikaz presretnutih zahtev i odgovora

Nakon što su zahtevi presretnuti i sačuvani u poseban fajl, mogu biti iskorišćeni unutar *SQLMap* alata. *SQLMap* pruža širok spektar automatizovanih testova i napada, ovo su neki od njih izvršeni prilikom testiranja naše aplikacije:

* Izlistavanje svih dostupnih baza unutar naše aplikacije  
  sqlmap -r C:\Users\user\Desktop\request.txt --dbs
* Izlistavanje svih tabela u bazi podataka  
  sqlmap -r C:\Users\user \Desktop\request.txt –D bezbednostDB --tables
* Izlistavanje kolona u tabeli (provera da li su lozinke enkriptovane)

sqlmap -r C:\Users\user \Desktop\request.txt –D bezbednostDB –T users

--columns

* Pokušaj izvršavanja proizvoljnih SQL upita

sqlmap -r C:\Users\user \Desktop\request.txt –D bezbednostDB –T users

--sql-query“UPDATE users SET password = ’123456’“

* Pokušaj brisanja tabele

sqlmap -r C:\Users\user \Desktop\request.txt –D bezbednostDB –T users

--dump

* Izvršavanje velikog broja automatizovanih testova za proveru sigurnosti baze podataka sa različitom agresivnošću (--risk) i dubinom testiranja

(--level)

sqlmap -r C:\Users\user \Desktop\request.txt --level=2 --risk=3

Nakon izvršavanja svih testova i napada došli smo do zaključka da naša aplikacija i baza podataka nema ulaznih tačaka koje su podložne SQL injekciji i da zadovoljavaju standarde bezbednosti *SQLMap* alata.